IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH CELL PHONE NUMBER 971-468-5287 THAT IS STORED AT PREMISES CONROLLED BY T-MOBILE US, INC.	Case No. 2:24mj877-CMR

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Melissa Hulls, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by T-Mobile US, Inc. ("T-Mobile"), a wireless provider headquartered at 4 Sylvan Way, Parsippany, NJ 07005. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require T-Mobile to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Park Ranger with the National Park Service ("NPS") within the Department of the Interior. I attended the Federal Law Enforcement Training Center ("FLETC") and graduated from the Land Management Police Training program and was certified in the field through the Field Training Evaluation Program administer by FLETC. I have been employed by the NPS in a law enforcement capacity since 2003, and have worked in Utah, California,

Arizona, Mississippi, and Washington. I have attended multiple law enforcement trainings and resident courses, including courses on the Archaeological Resource Protection Act, Standardized Field Sobriety Testing, REID Technique of Investigative Interviewing and Advanced Interrogation, NPS Law Enforcement De-Escalation, Verbal Judo, Resource Law, Report Writing, and more.

3. I am working in this capacity to locate a missing hiker in Arches National Park.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 36 CFR §§ 2.10(a), 13.25 (Camping Overstay) have been committed by Francis Userovici.[1] There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

[1] See also 18 U.S.C. § 1865(a) (proscribing a term of imprisonment of up to six months for violation of regulations relating to the use and management of a national park).

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On August 16, 2024, at approximately 8:50 AM, the National Park Service recorded Francis Userovici entering Arches National Park based on video camera footage at the main park entrance. He was observed driving a Black 2024 Mercedes C300, 4-Door Sedan, with Arizona Plate No. CWD1911.

8. The same vehicle was observed by law enforcement officers at the Sand Dune Arch parking lot on August 23, 2024, and has not moved since.

9. Law enforcement officers determined that Mr. Userovici stayed at the Days Inn in Moab, Utah on the night of August 15–16, 2024, and was supposed to check out on September 17, 2024, but did not. This information was obtained from Days Inn based on exigent circumstances surrounding Mr. Userovici's disappearance.

10. Hertz Car Rental confirmed that Mr. Userovici rented the Black 2024 Mercedes C300, 4-Door Sedan during the rental period based on these exigent circumstances.

11. With the assistance of the Investigative Branch Services of the National Park Service, Mr. Userovici's telephone number was identified as 971-468-5287, which was further determined to be a "burner" phone. Mr. Userovici's family confirmed this phone number was obtained by Mr. Userovici after the family arrived in the United States from France, with the purpose of communicating throughout the duration of his trip.

12. Law enforcement officers have scoured the area surrounding the Sand Dune Arch parking lot but have not been able to locate Mr. Userovici, despite the use of aerial surveillance and K-9s. His family has confirmed that he is missing, with his last known location being Arches National Park.

13. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for T-Mobile subscribers may be located on the computers of T-Mobile. Further, I am aware that computers located at T-Mobile contain information and other stored electronic communications belonging to unrelated third parties.

14. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of T-Mobile for weeks or months.

15. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by T-Mobile for short periods incident to and following their

transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

16. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

17. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique

identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

18. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

19. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

20. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well records of any actions taken by the provider or user as a result of the communications.

21. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider

may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require T-Mobile to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

23. Based on the forgoing, I request that the Court issue the proposed search warrant.

24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

25. The government will execute this warrant by serving the warrant on T-Mobile. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted:

/s/ Melissa Hulls
Melissa Hulls
Park Ranger
National Park Service

Subscribed and sworn to before me on August 30, 2024

Cecilia M. Romero
_____
HON. CECILIA M. ROMERO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with cell phone number 971-468-5287 that is stored at premises owned, maintained, controlled, or operated by T-Mobile, a wireless provider headquartered at 4 Sylvan Way, Parsippany, NJ 07005.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by T-Mobile

To the extent that the information described in Attachment A is within the possession, custody, or control of **T-Mobile**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **T-Mobile** or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **T-Mobile** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All voice mail, text, and multimedia messages from August 16, 2024 at 8:00 AM to August 24, 2024 at 11:59 PM, stored and presently contained in, or on behalf of the account or identifier;

b. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from August 16, 2024 at 8:00 AM to August 24, 2024 at 11:59 PM;

c. All information about the location of cell phone number 971-468-5287 from August 16, 2024 at 8:00 AM to August 24, 2024 at 11:59 PM. This includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well

as all data about which "cell towers" (*i.e.*, antenna towers covering specific geographic areas) and "sectors" (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

The Provider is hereby ordered to disclose the above information to the government within **48 hours** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 36 CFR §§ 2.10(a), 13.25 (Camping Overstay) since August 16, 2024, involving Francis Userovici, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

b. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

c. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [**PROVIDER**], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [**PROVIDER**]. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[PROVIDER]**, and they were made by **[PROVIDER]** as a regular practice; and

b. such records were generated by **[PROVIDER'S]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[PROVIDER]** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature